



# Mobile Security

**A non-technical opinion of mobile phone capabilities and  
their use to deliver secure remote transactions**

## **OWNERS**

Author – Greg Walter (CEO / Founder)  
Qpay Pty Ltd  
3/2 Pittwin Street North  
Capalaba Qld 4157  
Australia  
Telephone +61 7 3245 4066  
Fax +61 7 3390 3603  
E-Mail [greg.walter@qpay.com.au](mailto:greg.walter@qpay.com.au)



---

## **Terms of use:**

**The following contains logic employed by Qpay in the development of the processes selected to deliver Qpay Remote Mobile payments. The opinions expressed are those held by members of the Qpay team and are not third party validated.**

**This document is not intended to be disparaging of other processes nor competing technologies. It is intended for internal and partner use only in the consideration of architectural and regulatory development.**



---

## I. Introduction

The mobile phone has become the ubiquitous device of choice worldwide. In spite of different cultural, commercial and technical drivers in differing regions, the mobile phone universally rules supreme for communications and social interaction. The mobile phone is usually the one thing consumers ensure they have with them when you go out. Do you use voice, SMS, email or the mobile Internet? Does your mobile phone store and play your music files? Now consumers can do banking and Internet purchasing via the mobile phone and much more!

This creates a new world of opportunities - new opportunities for business to transact with their customers, for customers to send money to each other locally and overseas, for financial institutions to provide services to their customers and for criminals to find ways to steal money.

The ability for consumers to transact remotely has created new conundrums for financial institutions. How can a call centre know it is really you on the end of the phone when they are given your credit card details to pay for a purchase? How does the Internet merchant know it is really you buying their goods and services with your credit card? As we move to the new paradigm of remote purchasing via a mobile phone security is a major challenge.



Whilst vendors and telecommunications carriers alike promote the virtues of mobile commerce and especially remote mobile payments, financial institutions are deeply concerned about the new forms of potential fraud – and rightly so. With cyber crime not expected to peak before 2011 at 10 times the current level (according to Gartner) the mobile phone poses a new and higher level of threat than previous technologies due to the complexity of mobile communications and the lower level of intelligence and protection they possess (when compared with a PC).

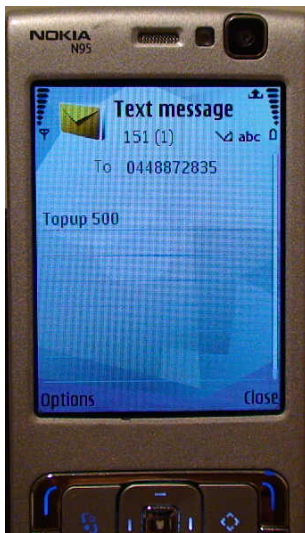
Add to this the emerging economies which will be mobile centric for banking and commerce; the need for highly secure solutions in the mobile space is clearly evident. If we cannot make a PC secure, how can we make a mobile phone secure for financial transactions? Even smart phones are much less intelligent than their PC peers.

This document considers the capabilities and limitations of the mobile telephone to securely conduct financial transactions, and provides opinions and recommendations to the design and architecture of the Qpay system.



---

## II. Three channels of challenges – SMS, Data and Voice



### SMS

In effect the mobile phone has three communication pipes attached – SMS, Mobile Internet and Voice. Each has different rules (protocols), functions and levels of secure ability.

When it comes to security, you want a certain degree of confidence that the device on the other end of your communication is really the mobile phone you believe it to be. The three channels represent varying degrees of certainty when you receive communications from the device, and when you send communications to the device.

**SMS receipt – simplest form of fraud.** For example, when you receive an SMS, there is usually a phone number at the top of the message. If you think you can be reasonably certain the SMS has come from the mobile phone number at the beginning of the message, you would be mistaken. It is very easy to provide a false number at the top of that SMS! In addition, it is very cheap to send bulk SMS messages via the Internet and pretend to be someone else! So if you are a criminal wanting to impersonate someone else, it is both simple and inexpensive to do so using SMS!

**SMS receipt methodology for fraud and subsequent risk analysis.** If people send SMS messages to a server to facilitate financial transactions, that server is an SMS recipient. Usually the messages received will contain an instruction and an identifier to enhance security – often in the form of a PIN. You may send “Pay 0448123456 50 1234” where 0448123456 is your friend’s mobile phone number and 1234 is your security PIN. This means you want to transfer \$50 to your friends account, and here is your PIN to prove you are really you.

If however a criminal were to send the server a text message “Pay 0449234234 50 1234” where the 0449234234 represent a criminal’s mobile phone account and 1234 is them guessing your PIN, then it would be cheap and easy for them to put your mobile phone number at the top of the message and pretend to be you.

Your PIN however gives you a certain level of insurance in this fraud attempt. A four digit PIN has 10,000 variables - 0000 to 9999. Most people use common PINs which means about 3,084 PINs are used most regularly, with 365 at the top of the list. These relate to dates of birth and cover every day of the year.

Most institutions give you three tries to get a PIN right before they lock your account. With the higher number of just over 3,000 variables, if a criminal tries your number three times,



they have a one in a thousand chance of getting it right (3,000 most common variables divided by three attempts). The risk profile is worse if you only take the 365 dates of birth. The risk profile of SMS messaging with a four digit PIN for security is therefore 0.1% conservatively (based on 3,000 odd most commonly used PINs, not 365). If you move to a six digit PIN, this drops to around three in 37,000. If you use a PIN which starts higher than 31, your risk profile drops by more than 50%!

The added problem is that if a criminal tries to guess your PIN and gets it wrong three times, your account gets locked. Once you unlock your account, the criminal can try again, and there is nothing your provider can do to stop them! So while your risk profile on a four digit PIN is 0.1% (or three in 37,000 for a six digit PIN), every time you unlock your account, the criminals can have another three tries to guess your PIN and steal your money!

### **Security profile of Single Layer SMS message with PIN:**

Four digit PIN Instant – 3 attempts x 3085 prime variables (conservative) = 0.1% success rate  
Four digit PIN over twelve month period (assuming a ten day PIN reset cycle) = 3.55% success

Six digit PIN Instant – 3 attempts x 37,000 prime variables (conservative) = 0.01% success rate

Six digit PIN over twelve month period (assuming a ten day PIN reset cycle) = 0.3% success rate

## **Mobile Data**

**Mobile Data / Mobile Internet / USSD risk profile.** Mobile phones have Internet access. Some vendors of mobile payments offer the ability for users to access payment functions over the Mobile Internet. This can be done many ways including the use of WAP, a simple protocol used by many less sophisticated mobile phones, the Mobile Web used by “smarter phones” and even with special software such as Java applications which can be very intuitive!



When a mobile phone accesses the Internet, the session is assigned a temporary IP address by their mobile phone operator. This address allows for the delivery of information to and from the mobile phone to other internet sites including the vendor’s site. To enhance security, the vendor will usually request the use of a password.

Most mobile phones cannot use secure encryption such as SSL (Secure Socket Layer). This means the information transmitted to the vendor’s server from most mobile phones can be easily viewed by criminals. For example, to intercept information which is not secured is simply a matter of putting a “sniffer” in one of the routers close to the Vendor’s server. Sniffers pick up information passing by and forward this information to the criminal’s servers.



<http://en.wikipedia.org/wiki/Sniffer> This is only one example of the many strategies criminals can employ to compromise information carries across the mobile internet.

Another way Mobile phones can be easily compromised on the mobile internet is with the use of malicious software. The first mobile phone virus was delivered in 2004 with numerous forms of malicious software now being engineered for smart phones – particularly on the Symbian and Microsoft Mobile operating systems. Just do a Google search on Mobile Virus to see the range of malicious software out there. Whilst the current count for very serious threats is less the 90 programs, the problem is that even smart phones are not smart enough to protect themselves from this threat. <http://www.viruslist.com/en/analysis?pubid=200119916>

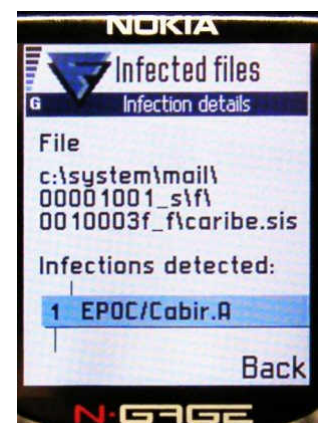
The use of the Mobile Internet for initiation and authentication of financial transactions – even by so called smart phones – is as fundamentally flawed as is the use of single layer e-commerce transactions without the use of anti-virus and very sophisticated security technology.

As antivirus protection for mobile phones increases a false sense of security is created. Even with the advent of data encryption on the mobile, fundamental vulnerabilities including keyloggers, root kits, Man-in-the-middle attacks will compromise this channel. Mobile phones are not as intelligent as PCs and laptop computers. Even so called “smart phones” do not come close. If we cannot currently guarantee the security of PC’s and laptop computers – even with sophisticated anti-virus software – how can mobile phones come close?

### **Blackberry mobile Internet:**

Blackberry represents another element to the mobile Internet equation as it can deliver a closed or private network transaction. There are two main drawbacks with this technology. One is the potential resistance for Financial Institutions to having their data go through a Blackberry server. This can be overcome by the Institutions providing their own closed Corporate Network access point to the user.

The other drawback to these private network solutions is when the customer goes to the open Internet, their device can be compromised by malicious mobile software (mobile malware). Items such as mobile keyloggers can then dump any private information into the criminal’s hands – especially as the use of closed networks for transactions creates overconfidence in this type of security. This overconfidence usually results in the use of a single layer authorization. All of the information required to perpetuate fraud is carried on this single layer and is therefore of very high value to criminals.



Copyright F-Secure Corp. 2004

### **Security profile of the Mobile Internet:**

Broadly, remote payments using single factor authentication such as username and password over the mobile internet has a substantially greater risk factor than a credit card transaction on a computer with no encryption and no virus protection.



---

## Mobile Voice

Using a mobile voice call to a computer server using voice to text recognition, a user could speak instructions (order requests for example) which could be captured by the IVR and processed. A PIN could also be spoken or entered using the mobile phone keypad during the call.

However, a single layer voice call for financial transactions is no less problematic than SMS, as you cannot guarantee the end user is really the end user. Many users block their call ID, and criminals could spam the server with computer generated voice calls attempting to hit on the PIN. This could be done relatively inexpensively using Voice over IP with a similar level of threat to SMS.

### **Security profile of Single Layer voice call from the user with PIN:**

Similar to SMS above but more expensive to form an attack.



---

### III. Generic technical strengths and limitations of the mobile platform

#### Phone identity.

When a mobile phone connects to the network, it is identified by a unique code in the SIM card. A special encryption code is then established for communications within the network. Communications within the network on a mobile phone are therefore fairly well secured for normal communications.



#### Hacking the network.

It is possible to break this security by the use of a fake base station \*. This process is easier than decoding 128Bit encryption over the internet. Listening to information this way for a long time would provide a criminal a wealth of information as financial transactions across the mobile become more commonplace. This could open the door to large scale (high volume) fraudulent attacks when accompanied with a process called SIM cloning.

#### Comparative security.

Whilst this is more difficult for a criminal to set up than to intercept information over the open Internet, most security analysts agree the use of the mobile phone security process alone is not adequate for the carriage of sensitive information. Other supporting technologies such as Transaction Anomaly Detection (TAD), information partitioning and the use of Multifactor authentication should be deployed in concert with Mobile transaction.

#### Information carried beyond the network.

Once information passes out of the mobile domain, it is then subject to the rules and security levels of the new domain. For example a mobile phone on the Internet has good security for normal communications within the mobile network environment, but when the communications passes to the open Internet, then that information is subject to the weaknesses of the Internet.

\* *Security And Embedded Systems* By Ran Giladi, Dimitrios Nikolaou Serpanos Page 189.

<http://books.google.com.au/books?id=KThliOe84PUC&pg=PA189&lpg=PA189&dq=mobile+phone+security+fake+base+station&source=web&ots=rIuK2vDi3L&sig=BEgIXbLVcLRGdwXFaGs55UCsNoo&hl=en#PPA189,M1>

<http://www.cs.stevens.edu/~swetzel/publications/mim.pdf>



---

## IV. The alternatives to single device / single layer / single session

### Single Factor.

A single factor, single layer single session transaction is where the transaction request / initiation and the security measure (such as a PIN) are conducted on the same device, same channel and in one session. Examples of these are an SMS with a PIN or an internet session with a password. Each of the analyses in section 2 above were based on this process.

It is generally agreed a single factor transaction from a mobile phone using SMS mobile data or mobile voice is inadequate to provide any level of confidence. None of these technologies on their own can provide a level of security even close to an online transaction using a PC with SSL encryption and virus protection.

This then requires that multiple factors, multiple channels and / or multiple sessions should be used for authentication to provide an adequate degree of certainty.

### Multifactor.

Multi Factor can overcome the limitations of single factor and reduce risk to varying degrees. Token is perhaps the most well known form of multifactor security. However, multifactor covers a wide range of solutions and architectures. It could be in the form of multiple devices (such as tokens), multiple channels, multiple sessions or a combination of these. Each technology delivers varying degrees of security, convenience, management and cost for mobile transactions.

### Multi-device.

A multi-device transaction is where two **devices** are used such as in the use of a PC to initiate a transaction and a token with a rolling password for authentication.



The mobile phone is centric to this paper, so the mobile would be one of the devices in a multi-device session. Other devices could include USB certificates (a certificate on a USB memory stick), Chip and PIN devices and tokens.

### Multi-channel.

A multi-channel transaction is where differing communications **channels** are used on the same media / device. The use of the SMS channel to initiate a transaction with the mobile phone voice channel to approve would be a multi-channel transaction. In this example:

1. The SMS channel from the user to the transaction server initiates the transaction
2. The mobile voice channel from the transaction server to the user's mobile phone authorizes the transaction

A multi-channel transaction is almost always multi-session (below).



---

### **Multi-session.**

A multi-session transaction happens when the initiation action and authentication action happen in two or more **sessions**. This would be the case if a transaction was initiated via SMS and the authentication was to happen via an SMS response from the transaction server. Multi-session could also happen via multiple channels. For example an SMS sent by the user could be authorized by a computer generated voice call. These processes are also usually referred to as multi-factor.



---

## V. Conclusion

In the mobile environment, a single layer communication (where both the initiation and the authentication actions are carried on a singular communications session) does not afford a level of security required for the carriage of sensitive (financial transaction) information. An SMS containing a transaction request and PIN is considered the weakest of these. A mobile Internet transaction protected by Username and Password is also weak and unsatisfactory.

It is highly recommended some form of multi-factor / multi-session or multi-device solution be employed for any form of financial transaction initiation, authorization or user identification. Failure to employ technologies beyond single factor, single layer single session transactions will result in substantial levels of fraud.

**Note:** This paper does not address the situation where both the initiation session AND the authentication session is compromised by a fake base station. This represents an equal playing field for all players and technologies in this arena (and is therefore not a fault in the aforementioned logic or recommendations within the competing technologies).